RISK ANALYSIS

Integrated Procurement System (Case Study)

U.S. Department of Housing and Urban Development

Month, Year

Revision Sheet

Release No.	Date	Revision Description
Rev. 0	1/31/00	SEO&PMD Risk Analysis
Rev. 1	5/1/00	Risk Analysis Template and Checklist
Rev. 2	6/14/00	Minor changes per Office of Administration

I have carefully assessed the Risk Analysis for the (System Name). This document has been completed in accordance with the requirements of the HUD System Development Methodology.

MANAGEMENT CERTIFICATION - Please check the appropriate statement.

_____ The document is accepted.

_____ The document is accepted pending the changes noted.

_____ The document is not accepted.

We fully accept the changes as needed improvements and authorize initiation of work to proceed. Based on our authority and judgment, the continued operation of this system is authorized.

_____	_____
NAME Project Leader	DATE
_____	_____
NAME Operations Division Director	DATE
_____	_____
NAME Program Area/Sponsor Representative	DATE
_____	_____
NAME Program Area/Sponsor Director	DATE

RISK ANALYSIS
TABLE OF CONTENTS

Page #

1.0 GENERAL INFORMATION

1.0 GENERAL INFORMATION

1.1 Purpose

In response to new Congressional reporting stipulations and amendments to FASA, OFPPA and GPEA requirements, the Office of Procurement and Contracts has instituted modifications designed to streamline its procurement and acquisition process. To better support these changes, the office is proposing to develop and deploy an integrated procurement system to replace its existing procurement system. Implementation of the proposed system has security implications that span data integrity, user and network access, et al. This risk analysis is aimed at evaluating the security threats and vulnerabilities that impact the successful development and operation of the proposed system. This analysis is also intended to identify appropriate countermeasures and mitigation strategies that should be put in place as part of this project's implementation activities.

1.2 Scope

The scope of this security analysis is centered on developing a sound and appropriate risk analysis methodology, and assessing the physical security and risks arising from natural, environmental, and human causes associated with the implementation and operations phases of the new Integrated Procurement System. The scope of the analysis includes a review of current and proposed hardware and software resource inventories, internal controls such as backup procedures, current contingency or disaster recovery plans, critical business applications and functions, operations interdependencies and criticality, potential interruptions, and recovery priorities.

This security risk analysis defines potential types of threats and the potential adverse impact should the threat event occur. Through a matrix format, the threats are mapped to associated vulnerabilities, likelihood of occurrence and potential damage in the event the threat should be realized (see Table 1 in section 5). A security risk factor is generated for each threat and recommended countermeasure(s) are defined.

1.3 System Overview

The Procurement and Contracting Office at Headquarters and the Regional Administrative Offices are responsible for administering the Department's procurement and acquisition process and are the organizations that will share responsibility for the Integrated Procurement System (IPS). IPS will utilize client server architecture to integrate procurement workflow and will be designed to support web-enabled access. This system is a major application that is designed to support and integrate procurement and acquisition processing activities.

The IPS production environment is described below:

Computing Requirements	Estimated Size	Basis
Personal desktop computer (PC)	CPU: Intel Pentium 133 MHz O/S: Modified MS Windows 95 RAM: 32 MB Local storage: 500 MB	One per User (HUD employee)
Access to SQL Server	1 gigabyte storage	Contractor Team Leader, developers, Procurement System users
Current Procurement System Software access	Icon; 100 bytes storage	Each Procurement System user
LAN Servers	25 MB space on each; 20 MB for application; 5 MB for contingency	Procurement System on production server

1.4 Project References

- Federal Acquisition Streamlining Act (FASA) of 1994
- Office of Federal Procurement Policy Act (OFPPA) of 1988
- Government Paperwork Elimination Act (GPEA) of 1998
- Office of Federal Procurement Policy Act Amendments of 1988 (Public Law 100-679)
- HUD System Development Methodology (SDM)
- The current procurement system's Software Quality Assurance Plan
- The current procurement system's Software Configuration Management Plan
- Procedure for Reviewing Project Commitments to External Individuals or Groups with Senior Management
- Procedure for Developing the Software Development Plan
- Procedure for Estimating the Size of the Project Software Work Products
- Procedure for Assessing the Project Critical Computer Resources
- Procedure for Deriving the Project Schedule
- Procedure for Revising the Software Development Plan
- Procedure for Reviewing External Project Commitments and Changes with Senior Management
- Powerscript Coding Standards and Naming Conventions

1.5 Terms and Abbreviations

Acronym/Abbreviation	Definition
CM	Configuration Management
OPC	The Office of Procurement and Contracts.
FAD	Field Accounting Division.
FOIA	Freedom of Information Act.
FPDC	The Federal Procurement Data Center.
FPDS	The Federal Procurement Data System maintained by the FPDC.
FRD	Functional Requirements Document.
GAO	General Accounting Office
Government	U. S. Government or Federal Government unless otherwise indicated.
GSA	General Services Administration
GTM	Government Technical Monitor.
GTR	Government Technical Representative.
IPS	Integrated Procurement System
JFMIP	Joint Financial Management Improvement Program
GUI	Graphical User Interface.
OFPP	Office of Federal Procurement Policy within OMB.
OIG	Office of Inspector General
OIT	Office of Information Technology.
OMB	Office of Management and Budget within the Executive Office of the President.
Program Office	The Office within the Department that initiates and has primary responsibility for, or interest in, a Procurement of property or services.
SQL	Structure Query Language.
QA	Quality Assurance
SDM	System Development Methodology.
RAD	Rapid Application Development.
WBS	Work breakdown structure.

1.6 Points of Contact

1.6.1 Information

The following persons can be contacted with questions pertaining to this document:

- Linda Williams, Project Leader, Office of Procurement and Contracts
- Robert Hawley, Project Leader, Office of Procurement and Contracts
- John Moriani, Configuration Manager, Office of Procurement and Contracts

1.6.2 Coordination

The following organizations must perform the following activities to ensure the successful development and deployment of the new IPS system:

- Office of Procurement and Contracts (OPC) (Headquarters and 25 Field Offices)
- Office of Information Technology (OIT)
- OPC Contractors

Organization	Coordination Activities	Associated Schedule
OPC	Planning, Project Management	03/07/FY00 – 02/28/FY01
OPC, OPC Contractors	Business Requirements Support, Systems Requirements Support	06/10/FY00 – 07/10/FY00
OPC Contractors	Systems Design and Analysis	06/30/FY00 – 08/30/FY00
OIT, OPC, OPC Contractors	Hardware/Software Acquisition and Integration	06/30/FY00 – 08/15/FY00
OPC Contractors	Development, Development Coordination	08/15/FY00 – 12/31/FY01
OIT, OPC Contractors	System Integration and Testing	01/01/FY01 – 02/01/FY01
OPC Contractors, OIT	Installation, Deployment and Training	02/01/FY01 – 02/28/FY01

2.0 PROJECT AND SYSTEM DESCRIPTION

2.0 PROJECT AND SYSTEM DESCRIPTION

2.1 Summary

The Integrated Procurement System (IPS) will incorporate web-based features and expanded data storage and archiving capabilities required to bring the agency into compliance with updates to FASA, OFPPA procurement processing and Congressional reporting requirements as well as GPEA stipulations. The system will be designed to provide the following capabilities:

- Automation of the high volume, low-dollar value simplified acquisition business processes performed in all Headquarters and field offices with delegated procurement authority.
- Standardization of business processing for over 5,000 annual HUD purchase order transactions for the entire simplified acquisition business cycle of small purchase requisition, solicitation production, purchase order production, and management reporting.
- Dual entry of the small purchase transactions in procurement and financial systems is eliminated by the IPS interface to the Department's central accounting system
- Staff performing simplified acquisitions in more than 25 locations have a standardized and fully automated system for purchase requisition, solicitation and a standardized and fully automated system for purchase requisition, solicitation, award, administration, and reporting..
- Program staff nationwide will be able to enter requests for contract services on-line as well as check status of submitted requests and generate reports.
- The Department will be better able to provide timely and accurate reports on Contracting activities to HUD management the Federal Procurement Data Center (FPDC), Office of Management and Budget within the Executive Office of the President (OMB), Congress, and the public.

The project is estimated to be a 9-month systems development effort and provide a useful system life of at least 5 years. The Department's Office of Information Technology will provide system development, maintenance and post-implementation support. Users will comprise the Department's employees with restricted access to vendors and members of the general public.

2.1.1 Project Management Structure

The Procurement and Contracting Office at Headquarters and the Regional Administrative Offices are responsible for administering the Department's procurement and acquisition process and are the organizations that will share sponsorship of the Integrated Procurement System (IPS). Mr. John Wright will serve as project leader on behalf of the sponsoring offices. The project's estimated start and end dates are June of FY00 through April of FY01.

2.1.2 Project Staffing

Determine the approximate number of staff hours required (HUD personnel and contractors) and identify the expertise, knowledge, skills, and abilities needed by the project team to develop and/or maintain a quality application system. Staff hours should be broken down by major skill category, both technical and program related. This information will help management determine the resources required and when they are needed.

Team Member Role and Labor Category	Estimated Hours	Responsibilities
Mary Hemmings Project Coordinator Labor Category: Senior Task Manager 4 Contractor	200	- Monitor and manage the overall status of the project - Assign responsibility for specific work products and tasks - Interface with client to discuss project requirements and schedules - Produce Project Management deliverables - Validate that all work is performed in accordance with SDM guidelines - Quality assurance - Develop the software development plan - Negotiate project commitments - Assist in analyzing the user requirements - User support of all the systems - Facilitate user assistance
Peter Samuel Team Leader/Business Analyst Sr. Technical Consultant 3A Contractor	780	- Lead the development team - Assist in designing, developing and implementing the work products - Develop, analyze and manage user requirements - Assist in developing and updating all SDM documents - Develop stored procedures on SQL server - Maintain SQL database for - Assist Task Leader in managing the project - Assign responsibility for specific work products and tasks - Provide technical support for - Quality assurance

Team Member Role and Labor Category	Estimated Hours	Responsibilities
Gavaskar Vengesum Programmer/Analyst Journeyman Programmer Analyst 4 Contractor	400	- Assist in analyzing, designing, developing and implementing - Provide technical and user support for - Perform system testing -
Parvesian Parveen/ Task Leader/Sr. Programmer/ Analyst Technical Consultant SA Contractor	690	- Assist in analyzing, designing, developing and implementing - Provide technical and user support for - Perform system testing
Venesh Vonteru Sr. Programmer/Analyst Sr. Technical Consultant 2 Contractor	400	- Assist in analyzing, designing, developing and implementing - Provide technical and user support for - Perform system testing
Lucy Lou Sr. Programmer/ Analyst Sr. Technical Consultant 2 Contractor	400	- Assist in analyzing, designing, developing and implementing - Provide technical and user support for - Perform system testing
Veronica De Forester Programmer/Analyst FTE	150	- Assist in analyzing, designing, developing and implementing - Provide technical and user support for - Perform system testing
Terry Patton Sr. Programmer/Analyst FTE	840	- Assist in analyzing, designing, developing and implementing - Assist in analyzing user requirements - Assist in conducting unit testing - Provide technical and user support for - Assist in developing and updating test plans - Perform system testing
Sharon Malaysia Sharon Programmer/Analyst FTE	250	- Assist in analyzing, designing, developing and implementing - Assist in analyzing user requirements - Assist in conducting unit testing - Assist in developing and updating test plans - Provide technical and user support for - Perform system testing

Team Member Role and Labor Category	Estimated Hours	Responsibilities
Pawtan Dhir Sr. Systems Analyst Sr. Technical Consultant 2A Contractor	1,400	- Analyze project procedures - Write project procedures - Analyze system errors, recommend fixes - Recommend system improvements - Quality assurance - Provide assistance to develop and update documents for - Assist in development of the Software Development Plan - Perform system testing
Jean Bonner Technical Writer/Analyst Technical Writer 3A Contractor	300	- Develop and update all the documents in accordance with SDM guidelines including User Manual for - Assist in developing and updating the FRD, System Specs, Program Specs, and Database Specs - Assist in developing and updating the System Test Plan and User's Manual - Assist in analyzing user requirements - Assist in analyzing, designing, developing and implementing - Develop and update the documents for - Perform system testing
John Moriani Configuration Manager Principal Tech. Consultant Contractor	1,945	- Ensure compliance to the SDM guidelines - Audit project to ensure compliance - Maintain configuration control for project deliverables
Stephanie Colin Project Leader FTE	760	- Ensure compliance to SDM guidelines - Audit project to ensure compliance - Maintain configuration control for project deliverables

2.2 Risk Management Structure

IPS maintains security and data integrity by allowing only users who possess valid combinations of User Ids and Passwords to access the system. The users, whether external users or HUD staff, are allowed access to only those program areas and functions that have been requested and approved by IPS Security Administrator at HUD Headquarters in accordance with IPS Security Procedures. These management controls include:

- Assignment of Security responsibility

- Application Rules
- Specialized Training

Assign Security Responsibility. Security responsibilities are assigned to two separate individuals as follows:

1. Management controls are assigned to an individual who has authority and resources to ensure that the selected management controls are implemented, and

2. Technical controls are assigned to a technically capable individual who has system administrator-level access and can ensure that the selected controls are implemented within the IPS application.

Application Rules. Establish a set of rules concerning use of and behavior within the application. The rules shall be as stringent as necessary to provide adequate security for the application and the information in it. Such rules shall clearly delineate responsibilities and expected behavior of all individuals with access to the application. In addition, the rules shall be clear about the consequences of behavior not consistent with the rules.

Specialized Training. Before allowing individuals access to the application, ensure that all individuals receive specialized training focused on their responsibilities and the application rules.

IPS will be shared by all major components of the Department. Each program area and the Office of Chief Procurement are responsible for their data within the database and share responsibility of functional subsets of the automated system. The

2.3 Periodic Risk Assessment

Notwithstanding a review by designated Security and System Administrators, periodically, as defined, CPO and CFO management will independently review the IPS Master Table Inquiry (MTI) log to ensure that only designated Security Administrators are controlling updates to users access rights and profiles on IPS Security Table. In addition, selected Security Table may be reviewed to ensure the existence of documentation for management approval or notification.

The security requirements will need to be updated regularly to adjust to newly discovered security holes and changes in system activity patterns. This may be to simply update the Security Monitoring software on a regular basis.

2.4 Contingency Planning

The contingency Plan will be routinely updated for responding to a system emergency. This includes performing backups, preparing critical facilities that can be used to facilitate continuity of operations in the event of an emergency, and recovering from a disaster.

Backup and contingency plans are included in the HUD Disaster Recovery Plan. The Office of IT (Admin. IT) has a hardware full-capacity replacement for all of HUD's computer applications. The IPS application will also be backed up daily and a duplicate copy is being kept at the Reston Data Center. A one-month recovery of these files is possible. Prior to the new software being put into production, a copy of new/revised source programs are copied and stored with a reputable data storage vendor.

3.0 SYSTEM SECURITY

3.0 SYSTEM SECURITY

Introduction

Security safeguards are an integral part of the development process of all HUD information systems. Security considerations and safeguards are to be described for new systems and/or modifications to existing systems in accordance with the requirements identified under HUD Handbook ADP Security Program. The security plan is prepared to include the security safeguard requirements for the new user interface on IPS web feature.

The mission critical elements of IPS are derived from IPS ability to maintain public confidence in terms of confidentiality of data, security, accuracy of data, and timeliness of reports. It is therefore crucial for the IPS to ensure that data is demonstrably protected and controlled. This perspective has produced this risk assessment and security plan to be conducted on the potential vulnerabilities incurred by the proposed new Integrate Procurement System.

General Description/Purpose

In keeping with the Federal Acquisition Streamlining Act (FASA) (1994), the Office of Procurement and Contracts has instituted a formal streamlined procurement and acquisition process. This process is currently supported by a standalone system that automates data collection as well as user interaction and access at various points in the procurement process workflow. Recent updates to FASA, amendments to the Office Federal Procurement Policy Act (1988), and new Congressional reporting requirements advocate the need for cross-functional integration of procurement activities and an expansion in the scope of data reporting and retention requirements. The functional and technological limitations of the current procurement system articulate the need to replace it with a more technologically and functionally capable application in order to facilitate compliance.

The Procurement and Contracting Office at Headquarters and the Regional Administrative Offices are responsible for administering the Department's procurement and acquisition process and are the organizations that will share responsibility for the proposed system — the Integrated Procurement System (IPS). IPS will utilize client server architecture to integrate procurement workflow and will be designed to support web-enabled access. This system is a major new application that is designed to support and integrate procurement and acquisition processing activities.

The Office of Procurement and Contracts has a proposed technological solution intended to facilitate its compliance with the above-mentioned legislative changes. This solution involves implementing a new Integrated Procurement System to replace the existing procurement system current in use by this office. This Feasibility Study assesses the viability of implementing this new

solution as a precursor to determining the project's scope and funding requirements. The objective of this Feasibility Study is to evaluate whether the proposed IPS system is the appropriate investment option.

3.1 Baseline Security Requirements

The following is a brief description of the components of IPS environment and their security requirements.

1. **Public Access via Internet.** Procurement Administrator will use a desktop PC equipped with web browser software (Netscape or MS Internet Explorer) to access IPS through Secure Systems. Secure Systems is the front-end security that allows access of HUD's trusted business partners to HUD's systems through the Internet.

2. **HUD Access via LAN/WAN.** Headquarters and filed office users will use their desktop PCs to access IPS via the HUD LAN/WAN environment mainly for requisition submission and reporting.

3. **Row Matrix.** Data Access will be controlled by the Secure Connect (Netscape Enterprise Web Server) security using roles. User roles are defined as a set of privilege associated with specific functions or tasks that an individual may perform. Roles will be assigned to each authorized person to permit that person to perform specific tasks.

4. **SQL Database Server.** The database server will require appropriate security controls to ensure adequate protection of the functions and associated data.

5. **Encryption/Digital Signature.** Encryption for the system includes the following user groups:
   HUD Users: HUD users are mainly HQ staff that is able to access the system using respective authorized login ID's. This requires encryption of passwords and user ID's. The passwords are alphanumeric, 6-character, and have a letter prefix (C-contractor, H-HUD Staff)
   Business Partners/Contractors: HUD business partners are external users who are to access the system through the Internet. This requires encryption of passwords and User ID's. User ID's and passwords for these users are controlled through Secure Systems security.

6. **Headquarters LAN/WAN/Firewall System**. A security plan for the LAN/WAN/Firewall System is to be prepared (by the infrastructure group) external to this plan and should address the Secure-Connect.

3.2 Baseline Security Safeguards

The Integrated Procurement System resides and operates in the HUD client-server environment on a Local Area Network (LAN). A designated System Security Administrator through user authentication and verification techniques controls user access. Further, functional access is granted on as-needed basis, as defined for job descriptions by program area supervisors in each program area. This ensures separation of duties and provides data integrity through the system. Microsoft SQL Server Database and software are maintained and executed on Windows NT servers operated by Lockheed-Marti Corporation at HUD Headquarters' data center. All application users and developers access the system from workstations connected through local area network routers to the NT platform. The general public does not have access to IPS.

A Windows NT 4.0 Server (NTIPSOPS), located at headquarters, is used for production operation. The system development is on Windows NT 4.0 Server (NTIPSDEV) also at headquarters. HUD operates this equipment through a contract with Lockheed Martin.

3.3 Sensitivity Level of Data

Description of IPS Information Sensitivity

IPS contains vital departmental financial data, contract, vendor's pricing and customer data. IPS will be handled hundreds of millions of dollars annually. Processing must be protected against fraudulent, duplicated and misdirected activities. Data must be secured against unauthorized access to ensure the integrity of the data and processed.

Protection Requirement

Table III-1 below indicates the risk and magnitude of harm – in ratings of HIGH, MEDIUM, LOW -- that could result from the loss of Confidentiality (disclosure), Integrity (modification/misuse), or Availability (destruction/denial) of IPS information.

Availability: The Integrated Procurement System must be operational when users need it, and the response time must be reasonable. IPS is scheduled to be available Monday through Friday from 7:00 a.m. to 8:00 p.m. EST – with reasonable response time. The level of risk and the resulting magnitude of harm resulting from the system not being available to users, or too slow to use effectively, is ranked as HIGH. The unavailability of the system may be caused by risks/events such as hardware/software failures, system disruption, virus attacks and even minor disasters – a water leak in the vicinity of the IPS system area.

The lack of system responsiveness may be caused by such factors as insufficient hardware, configuration issues, or too many users for the design of the system. Downtime, particularly during normal working hours, will impact the performance of work and may cause work stoppages in some cases. Thus, the risk and magnitude of harm can be directly estimated in real dollar losses. Commensurately, the IPS Web Interface will be designed with a high degree of availability (i.e. hardware redundancy and backup) and will have the required contingency/backup plan, properly testes.

Integrity: The Integrated Procurement System must provide reasonable protection against the unauthorized modification of data within the system. The risk and magnitude of harm that could result from unauthorized modification of data is ranked HIGH. The loss of integrity can be the result of intentional (e.g. fraud, abuse) and unintentional acts (e.g. mistakes, errors, and omissions). The integrity issue is considered to be HIGH for Headquarters and Field Offices because of the higher-level privileges that these users normally require.

Confidentiality: The risk and magnitude of harm from unauthorized disclosure of IPS data is rated as HIGH. Virtually all of the data becomes (or can become) public at some point, although there may be some risk in the timing of data released to the public.

Table III-1 provides risks and magnitude of harm for the associated protection requirements for IPS system.

Protection Requirements	Risk and Magnitude of Harm		
	HIGH	MEDIUM	LOW
Availability of System	Ö		
Integrity of Data	Ö		
Confidentiality of Data	Ö		

Table III-1: Risk and Magnitude of Harm

Input/Output Controls (Integration with Other Systems)

IPS will be released to the Computer Services Group of OCIO for production. IPS will have operations manual that identifies all batch operations needs to be performed for all processing cycles. Before the release of each module, detailed operational instructions will be provided in the form of IPS run book. The manual identifies all operations, inputs, outputs, application backup and recovery procedures and schedules, and other required resources. IPS users will control all interactive input and generated output. Printed material will normally be printed in or delivered to the user's work area.

The following lists the input requirements and output capabilities of the proposed system requirements:

Inputs:

- Capability that allows for the interface to the Department's central accounting system to enable the dual entry of the small purchase transactions
- Capability that allows Program Staff nationwide to enter requests for contract services
- Capability to provide activity-tracking screens for collecting funding and vendor data elements
- Online, offline and remote data entry capability for staff in 25 Field Office locations
- Capability that enables the capture all of the data required to complete the following HUD Forms:
- FPDS SF 281 and 279 Report
- HUD 10.4, Requisition for Supplies, Equipment, Forms, Publications and Procurement Services
- SF-18, Request for Quotations
- SF-30, Amendment of Solicitation/Modification of Contract
- OF 347, order for Supplies or Services

Outputs:

- Capability to provide reports on contract status, status of submitted requests and generate regularly scheduled reports for Program staff nationwide
- Capability to generate timely and accurate reports on contracting activities to HUD management in the Federal Procurement Data Center (FPDC), Office of Management and Budget within the Executive Office of the President (OMB), Congress, and the public
- Capability to generate standardized management reports
- Capability to generate reports on data collected at each Action stage in the workflow

Security modules control individual users' access to querying funds and financial status, establishing or modifying an obligation sent to IPS. CA TopSecret, a security management software, controls individual user access to the production environment. The user is required to enter his/her unique user-id.

Interfaces:

VISA
PAYROLL
HUDCAPS
Program Accounting System (PAS)
HUD Procurement System (HPS)
Host-to-Host to US Treasury for disbursing

3.4 User Security Investigation Level and Access Need

All users of HUD computers and computer application software submit a HUD User Access Registration/Request Form. This form includes a certification by the user that they have read and will comply with the Departmental security guidelines. All users of IPS must complete and submit the appropriate IPS security access forms.

Forms must be signed b the user's supervisor and forward to the Office of Human Resources for certification that a National Agency Check Inquiry Level 1, background check has been performed on the user. Personnel authorized to grant access to the application and those empowered to approve will be subject to background investigation.

Restricting access will eliminate unauthorized access, by job function, to selected users identified by access codes and by holding users accountable for transaction attributable to tem. All attempts to access the system will be recorded and review by management on a regular basis.

Users are grouped together by functional area based on the type of system access required. This is done through the use of model security profile. Users with similar system access requirements may be linked to a model security profile. A model profile is an entry in the security table, which can be used by several users. All security profiles will be reviewed periodically.

4.0 RISKS AND SAFEGUARDS

4.0 RISKS AND SAFEGUARDS

The Computer Security Act requires that the safeguards be "commensurate" with the "risk and magnitude of harm" (i.e. a HIGH risk and magnitude of harm require a proportionately HIGH level of safeguards).

4.1 Risk and Security Safeguards Categories

Security measures and safeguards for IPS are grouped into three categories, Management and Development/Implementation and Technical, which are further broken down into subcategories. A brief description is provided for each subcategory. The detailed specifications (or controls) within for each subcategory is listed on the attached checklists, which also provide for the status of the control: In Place, Planned, or NA (not applicable) or NP (not planned).

4.1.1 Management Controls

IPS maintains security and data integrity by allowing only users who possess valid combinations of User Ids and Passwords to access the system. The users, whether grant recipients or HUD staff, are allowed access to only those program areas and function that have been requested and approved by IPS Security Administrator hat HUD Headquarters in accordance with IPS Security Procedures. Management Controls include:

- Assignment of Security responsibility
- Application Rules
- Specialized Training

Assign Security Responsibility. Security responsibilities are assigned to two separate individuals as follows:
(1) Management controls are assigned to an individual who has authority and resources to ensure that the selected management controls are implemented, and
(2) Technical controls are assigned to a technically capable individual who has system administrator-level access and can ensure that the selected controls are implemented within the IPS application.

Application Rules. Establish a set of rules concerning use of and behavior within the application. The rules shall be as stringent as necessary to provide adequate security for the application and the information in it. Such rules shall clearly delineate responsibilities and expected behavior of all individuals with access to the application. In addition, the rules shall be clear about the consequences of behavior not consistent with the rules.

Specialized Training. Before allowing individuals access to the application, ensure that all individuals receive specialized training focused on their responsibilities and the application rules.

- **Assignment of Security Responsibility – In Place**

Security is a shared departmental responsibility. The HUD IT Security Personnel has over-all control and the authority to delegate levels of control to developers, end users and operations personnel as needed.

The Office of Information Technology is responsible for establishing and controlling access to the development and testing environments. The operations staff is responsible for the security of the computer center, software and all data used or stored there.

- **Personnel Security – In Place**

All users of HUD computers and computer application software submit a HUD User Access Registration/Request Form. This form includes a certification by the user that they have read and will comply with the Departmental security guidelines. All users of IPS must complete and submit the appropriate IPS security access forms.

Forms must be signed b the user's supervisor and forward to the Office of Human Resources for certification that a National Agency Check Inquiry Level 1, background check has been performed on the user. Personnel authorized to grant access to the application and those empowered to approve will be subject to background investigation.

- **Independent Management Review – In Place**

Notwithstanding a review by designated Security and System Administrators, periodically, as defined, CPO and CFO management will independently review the IPS Master Table Inquiry (MTI) log to ensure that only designated Security Administrators are controlling updates to users access rights and profiles on IPS Security Table. In addition, selected Security Table may be reviewed to ensure the existence of documentation for management approval or notification.

4.1.2 Development/Implementation Controls

- **Security Specifications – In Place**

Stringent security requirements have been built into IPS. All security specifications are addressed in the system design document that was prepared during IPS system development. IPS exists in a controlled environment with access limited to authorized personnel for the purposes of testing, maintenance, supplemental development and operations.

- **Design Review and Testing – In Place**

The project sponsor and Program Office clients during their initial system development effort and each additional system enhancement reviewed IPS design. Test plans were developed and system software was user tested to ensure compliance with plan criteria.

- **Initial Authorization**

System sponsors and users certify software supplied or developed in each phase of the project before it is moved to the production environment. Certification, in memorandum form, is based on test plans for each user area that exercise all common system functions and those that are relevant to the particular program area. Independent validation and validation testing and user acceptance testing is performed on software developed to augment the initial IPS system, and documented in result reports.

4.1.3 Technical and Operational Controls

- **Physical and Environmental Protection – In Place**

The hardware used to develop, test and operate IPS is in a secure area under the control of Admin. IT. The workstations used to develop and access IPS are in HUD work areas with limited access. The work areas are kept locked during non-business hours. All environmental controls to protect hardware/software are documented under General Support Systems Plan.

- **Production Controls – In Place**

The following controls are operating over input, processing, and output data and media, and over access controls on the data and media with:

IPS Data Security -- Access to data with IPS is controlled by IPS program area and functional area. User ID controls access to IPS program and functional areas. IPS user may only work with information related to the program area and functional area he or she has been assigned.

Production I/O Controls – Before the release of each module, detailed operational instructions have been provided in the form of IPS run book. The manual identifies all operations, inputs, outputs, application backup and recovery procedures and schedules, and other required resources. IPS users will control all interactive input and generated output. Printed material will normally be printed in or delivered in the user's work areas. Each user area has procedures in place to control access to sensitive information produced by the system.

- **Business Resumption (Contingency) Planning – In Place**

Backup and contingency plans are included in the HUD Disaster Recovery Plan. The Office of IT (Admin. IT) has a hardware full-capacity replacement for all of HUD's computer applications. IPS application is backed up daily and a duplicate copy is being kept at the Reston Data Center. A one-month recovery of these files is possible. Prior to the new software being put into production, a copy of new/revised source programs are copied and stored with a reputable data storage vendor.

- **Application Software Maintenance Controls – In Place**

All IPS software will be maintained and backed up in a controlled environment managed by the Office of IT. Strict version control and user certification procedure will ensure the integrity of the software.

The Office of IT requires users to review and sign a Document of Understanding prior to system software modification. These documents specify the changes to be made to system and fully authorized system development/modifications.

PVCS, an integrated set of software configuration management tools used to automate, control and monitor the application development and maintenance process. PVCS manages and tracks all development and maintenance activity and provides for the automated movement of the application through the software development life cycle (SDLC). It maintains complete audit trail and version controls. All IPS baseline and IPS-specific source code will be migrated to PVCS.

All system proposed changes are processed by the IPS Change Control Board which operates in conjunction with the Financial Systems Integration project. All IPS system enhancements will need to be presented before the CCB to be vote and approve or disapprove. Cost estimates and impact analyses will also need to be presented for each suggested enhancement to assist the CCB in making its determination.

- **Documentation – In Place**

The following documentation is maintained:

Operational Guide/Manual
Training Manual
Systems Specification
Functional Requirements Document
Program Description and Specification
Data Dictionary

- **Security Training – In Place**

  OIT and OCIO provides periodic training in computer security awareness and accepted computer security awareness practices for all employees and contractor who develop, manage, operate and use Federal computer systems

5.0 COST AND EFFECTIVENESS OF SAFEGUARD

5.0 THREAT/VULNERABILITY/RISK/PRIORITY/COUNTERMEASURE MATRIX.

This risk assessment, Threat/Vulnerability Matrix, addresses identified vulnerabilities and threats to HUD environment, and specifies countermeasures for the individual threats and vulnerabilities. This risk assessment provides information on the overall security status. Specifically, it provides information on the existence and application of the security processes and policies. It is a cornerstone activity that must be repeated as often as necessary to maintain an accurate global assessment of the security status.

Risk #	Threat	Vulnerability	Potential Damage [low-1, med-2, high-3]	Likelihood [low-1, med-2, high-3]	Risk to HUD [damage x threat]	Cost to Fix	Priority	Countermeasure and Recommendation
Access Control *Section A*								
R-A.1	Network level access to Servers	Network level access to the Remote Servers will be required leaving the system vulnerable to IP based attacks.	2	3	6	1	6	NT Security; IP forwarding disabled; Advanced TCP/IP filtering; Latest NT Patches (Security Maintenance program); Turn off all unnecessary services;
R-A.2	Remote Servers must be remotely managed via the network	Remote management network traffic could be compromised and used to attack the Remote Servers via the network.	3	2	6	2	3	Domain password protection; Strict controls on remote users
R-A.3	Remote Dial backup to the routers is required	Dialup services are vulnerable to a variety of attacks	3	3	9	1	9	Follow client Dialup policy; Use Dialback functionality: Restrict Dialup access to emergency access only

R-A.7	Management Stations require high levels of access to devices on the network.	Unauthorized network access to these devices means unauthorized network access to all resources	3	2	6	2	3	Management stations to be located behind firewalls on secured network
R-A.8	Management Stations require high levels of access to devices on the network.	Logging & configuration information on management stations could provide enough information to compromise the network	2	2	4	1	4	Access into secured network restricted; Terminal access to management stations must be secured
R-A.11	TCP/IP Routing is used to direct network traffic	IP Traffic is vulnerable to IP spoofing (impersonation) attacks to falsify traffic	3	2	6	1	6	ACL's on participant and regional routers to check sources.
R-A.12	All systems require/have FTP access on the network	FTP Redirect attack can be performed to gain unauthorized FTP access	3	2	6	1	6	NetRanger Monitoring for this type of attack.
Physical Security *Section B*								

R-B.1	Remote Servers and components will be physically accessible in an uncontrolled environment	Physical access to the terminal represents the simplest means to obtain unauthorized access	2	3	6	3	2	Security Policies & Checklists; Partnership requirements; Locked Cabinet; Limited terminal access; snmp alerts of access to terminal and cabinet; SNMP alerts of change in link status; remote shutdown capabilities
R-B.3	Wiring from Remote Servers cabinet and resources are physically accessible on partner premises	Any exposed network wiring can be tapped and used to listen to all network traffic and therefore exposing sensitive data	2	3	6	2	3	Monitor Link Status; Strict Security Policies & requirements for partner environments;
R-B.4	Hub is physically accessible in an uncontrolled environment	The network is exposed to any party who wishes to listen to network traffic, impersonate other machines, and allows for bypassing critical network security	3	2	6	2	3	Use physical access controls (above); Disable unused ports; Monitor link status
R-B.5	Physical access to resources not controlled by HUD	Any component of the Remote Servers can be compromised using physical access	3	3	9	2	4.5	Security Policies & Checklists; Partnership requirements; Locked Cabinet, Physical access controls
Confidentiality and Integrity *Section C*								
R-C.1	Information stored on Remote Servers can be compromised	Unencrypted or unrestricted files and software could be read and or altered	2	2	4	1	4	Use NTFS with strict access control; Log filesystem changes; Monitor privileged users

R-C.2	Transactions over the network can be compromised	Transaction traffic contains confidential information that could be compromised	3	2	6	3	2	Encrypt Transaction traffic over WAN links
R-C.11	Encryption keys are exchanged and validated via the network	Keys can be captured or altered leading to compromise of the encryption mechanisms	2	2	4	2	2	x9.17 standard DES exchange - prefer x9.30 exchange if possible
R-C.14	Information is backed up remotely via the network	Information in backup files can be altered or used to compromise a system	2	2	4	2	2	Control access to backup and restore functions; Set strict permissions on files and directories pertaining to backup/restore
R-C.16	System logs are transmitted via the network	System logs can be altered or used to provide information to compromise a system	3	2	6	3	2	Encrypt log files over WAN links
Authentication Infrastructure *Section D*								
R-D.3	Windows NT is accessible via the network	Unauthorized access to the Windows NT OS can be obtained through the network	3	3	9	2	4.5	Require strong passwords and standardized account names, remove/disable unused accounts restricted access to system files; Use NT Domain Model
R-D.4	The NetRanger intrusion detection and management devices are accessible via the network	Unauthorized access to the NetRanger devices can be obtained through the network	3	3	9	2	4.5	Use strong OS authentication, complex passwords, encrypted password file in OS.
Security Logging and Audit Trails								

Section E								
R-E.1	Windows NT OS can be compromised using any of several means for unauthorized access	An incident, attack or loss of data could go unnoticed or without recourse	3	2	6	2	3	Maintain a database of dated and timestamped OS log files to provide a trail for auditing and event tracking
R-E.5	A preventable incident or attack can go unnoticed or happen without warning	An incident, attack or loss of data could go unnoticed or without recourse	2	2	4	2	2	Use SNMP traps to alert administrators to new events or incidents on the systems. This will alert for security attacks, special accesses etc.
Policy & Guidelines *Section F*								
R-F.1	Network resources and data can be compromised and or lost	Without declared preventative measures, actions for recourse, and incident recovery procedures, systems and data will be permanently lost	3	3	9	2	4.5	Have a complete set of policies procedures standards and guidelines for system, network and information security

6.0 RISK REDUCTION RECOMMENDATION

6.0 ADMINISTRATIVE PROCEDURES TO GUARD DATA INTEGRITY, CONFIDENTIALITY, AND AVAILABILITY

The following is a documented of IPS' formal practices to manage the selection and execution of security measures to protect data, and to manage the conduct of personnel in relation to the protection of data

Risk/Security		Implementation Recommendations ● = mandatory; ⊙ = at least one required; ○ = optional
Contingency plan (a routinely updated plan for responding to a system emergency, that includes performing backups, preparing critical facilities that can be used to facilitate continuity of operations in the event of an emergency, and recovering from a disaster)	● ● ● ● ●	**Applications and data criticality analysis** (an entity's formal assessment of the sensitivity, vulnerabilities, and security of its programs and information it receives, manipulates, stores, and/or transmits) **Data backup plan** (a documented and routinely updated plan to create and maintain, for a specific period of time, retrievable exact copies of information) **Disaster recovery plan** (the part of an overall contingency plan that contains a process enabling an enterprise to restore any loss of data in the event of fire, vandalism, natural disaster, or system failure) **Emergency mode operation plan** (the part of an overall contingency plan that contains a process enabling an enterprise to continue to operate in the event of fire, vandalism, natural disaster, or system failure) **Testing and revision procedures** (the documented process of periodic testing of written contingency plans to discover weaknesses and the subsequent process of revising the documentation, if necessary)

Risk/Security		Implementation Recommendations ● = mandatory; ⊙ = at least one required; ○ = optional
Information access control (formal, documented policies and procedures for granting different levels of access to health care information)	● ● ●	**Access authorization** (information-use policies and procedures that establish the rules for granting access; for example, to a terminal, transaction, program, process, or some other user) **Access establishment** (security policies and rules that determine an entity's initial right of access to a terminal, transaction, program, process or some other user) **Access modification** (security policies and rules that determine the types of, and reasons for, modification to an entity's established right of access, to a terminal, transaction, program, process, or some other user)
Internal audit (in-house review of the records of system activity (such as logins, file accesses, and security incidents) maintained by an organization).		

Risk/Security		Implementation Recommendations ● = mandatory; ⊙ = at least one required; ○ = optional
Personnel security (all personnel who have access to any sensitive information have the required authorities as well as all appropriate clearances)	● ● ● ● ● ●	**Assuring supervision of maintenance personnel by an authorized, knowledgeable person** (documented, formal procedures and instructions for the oversight of maintenance personnel when the personnel are near health information pertaining to an individual) **Maintaining a record of access authorizations** (ongoing documentation and review of the levels of access granted to a user, program, or procedure accessing health information) **Operating and maintenance personnel have proper access authorization** (formal documented policies and procedures for determining the access level to be granted to individuals working on, or near, health information) **Personnel clearance procedures** (a protective measure applied to determine that an individual's access to sensitive unclassified automated information is admissible) **Personnel security policies and procedures** (formal documentation of procedures established and maintained to ensure that all personnel who have access to sensitive information have the required authority as well as appropriate clearances) **Security awareness training** (assuring that system users, including maintenance personnel, receive appropriate security training)

Risk/Security		Implementation Recommendations ● = mandatory; ⊙ = at least one required; ○ = optional
Security configuration management (measures, practices, and procedures for the security of information systems that must be coordinated and integrated with each other and other measures, practices, and procedures of the organization established in order to create a coherent system of security)	●	**Documentation** (written security plans, rules, procedures, and instructions concerning all components of an entity's security)
	●	**Hardware and software installation and maintenance review and testing for security features** (formal, documented procedures for connecting and loading new equipment and programs, periodic review of the maintenance occurring on that equipment and programs, and periodic security testing of the security attributes of that hardware/software)
	●	**Inventory** (the formal, documented identification of hardware and software assets)
	●	**Security testing** (process used to determine that the security features of a system are implemented as designed and that they are adequate for a proposed applications environment; this process includes hands-on functional testing, penetration testing, and verification)
		Virus checking (The act of running a computer program that identifies and disables: 1) another ''virus'' computer program, typically hidden, that attaches itself to other programs and has the ability to replicate 2) a code fragment [not an independent program] that reproduces by attaching to another program 3) code embedded within a program that causes a copy of itself to be inserted in one or more other programs)

Risk/Security		Implementation Recommendations ● = mandatory; ⊙ = at least one required; ○ = optional
Security incident procedures (formal documented instructions for reporting security breaches)	● ●	**Report procedures** (documented formal mechanism employed to document security incidents) **Response procedures** (documented formal rules or instructions for actions to be taken as a result of the receipt of a security incident report)

Risk/Security		Implementation Recommendations ● = mandatory; ⊙ = at least one required; ○ = optional
Security management process (creation, administration, and oversight of policies to ensure the prevention, detection, containment, and correction of security breaches involving risk analysis and risk management; includes the establishment of accountability, management controls {policies and education}, electronic controls, physical security, and penalties for the abuse and misuse of its assets, both physical and electronic)	● ● ● ●	**Risk analysis** (a process whereby cost-effective security/control measures may be selected by balancing the costs of various security/control measures against the losses that would be expected if these measures were not in place) **Risk management** (process of assessing risk, taking steps to reduce risk to an acceptable level, and maintaining that level of risk) **Sanction policies and procedures** (statements regarding disciplinary actions that are communicated to all employees, agents, and contractors; for example, verbal warning, notice of disciplinary action placed in personnel files, removal of system privileges, termination of employment, and contract penalties; they must include employee, agent, and contractor notice of civil or criminal penalties for misuse or misappropriation of health information and must make employees, agents, and contractors aware that violations may result in notification to law enforcement officials and regulatory, accreditation, and licensure organizations) **Security policy** (statement(s) of information values, protection responsibilities, and organization commitment for a system as the framework within which an entity establishes needed levels of information security to achieve the desired confidentiality goals)

Risk/Security		Implementation Recommendations ● = mandatory; ⊙ = at least one required; ○ = optional
Termination procedures (formal documented instructions, which include appropriate security measures, for the ending of an employee's employment or an internal/external user's access)	● ● ● ●	**Changing locks** (a documented procedure for changing combinations of locking mechanisms, both on a recurring basis and when personnel knowledgeable of combinations no longer have a need to know or require access to the protected facility or system) **Removal from access lists** (physical eradication of an entity's access privileges) **Removal of user account(s)** (termination or deletion of an individual's access privileges to the information, services, and resources for which they currently have clearance, authorization, and need-to-know when such clearance, authorization and need-to- know no longer exists) **Turning in of keys, tokens, or cards that allow access** (formal, documented procedure to ensure all physical items that allow a terminated employee to access a property, building, or equipment are retrieved from that employee, preferably before termination)

Risk/Security		Implementation Recommendations ● = mandatory; ⊙ = at least one required; ○ = optional
Training (education concerning the vulnerabilities of the health information in an entity's possession and ways to ensure the protection of that information)	● ● ● ● ●	**Awareness training for all personnel, including management** (including, but not limited to, password maintenance, incident reporting, and viruses and other forms of malicious software) **Periodic security reminders** (employees, agents, and contractors are made aware of security concerns on an ongoing basis) **User education concerning virus protection** (training about the potential harm that can be caused by a virus, how to prevent the introduction of a virus to a computer system, and what to do if a virus is detected) **User education in importance of monitoring log-in success or failure and how to report discrepancies** (training in the user's responsibility to ensure the security of health care information) **User education in password management** (type of user training in the rules to be followed in creating and changing passwords and the need to keep them confidential)

6.1 Physical safeguards to guard data integrity, confidentiality, and availability

Requirement		Implementation features ● = mandatory; ⊙ = at least one required; ○ = optional
Assigned security responsibility (practices established by management to manage and supervise the execution and use of security measures to protect data and to manage and supervise the conduct of personnel in relation to the protection of data).		
Media controls (formal, documented policies and procedures that govern the receipt and removal of hardware/software [such as diskettes and tapes] into and out of a facility)	● ● ● ● ●	**Access control** **Accountability** (the property that ensures that the actions of an entity can be traced uniquely to that entity) **Data backup** (a retrievable, exact copy of information) **Data storage** (the retention of health care information pertaining to an individual in an electronic format) **Disposal** (final disposition of electronic data, and/or the hardware on which electronic data is stored)

Requirement		Implementation features ● = mandatory; ⊙ = at least one required; ○ = optional
Physical access controls (formal, documented policies and procedures to be followed to limit physical access to an entity while ensuring that properly authorized access is allowed)	●	**Disaster recovery** (the process enabling an entity to restore any loss of data in the event of fire, vandalism, natural disaster, or system failure)
	●	**Emergency mode operation** (access controls in place that enable an entity to continue to operate in the event of fire, vandalism, natural disaster, or system failure)
	●	**Equipment control** (into and out of site; documented security procedures for bringing hardware and software into and out of a facility and for maintaining a record of that equipment. This includes, but is not limited to, the marking, handling, and disposal of hardware and storage media)
	●	**Facility security plan** (a plan to safeguard the premises and building [exterior and interior] from unauthorized physical access and to safeguard the equipment therein from unauthorized physical access, tampering, and theft)
	●	**Procedures for verifying access authorizations before granting physical access** (formal, documented policies and instructions for validating the access privileges of an entity before granting those privileges)
	●	**Maintenance records** (documentation of repairs and modifications to the physical components of a facility, such as hardware, software, walls, doors, and locks)
		Need-to-know procedures for personnel access (a security principle stating that a user should have access only to the data he or she needs to perform a particular function)

Requirement		Implementation features ● = mandatory; ⊙ = at least one required; ○ = optional
Policy and guidelines on work station use (documented instructions/ procedures delineating the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific computer terminal site or type of site, dependent upon the sensitivity of the information accessed from that site)		
Secure work station location (physical safeguards to eliminate or minimize the possibility of unauthorized access to information; for example, locating a terminal used to access sensitive information in a locked room and restricting access to that room to authorized personnel, not placing a terminal used to access patient information in any area of a doctor's office where the screen contents can be viewed from the reception area)		
Security awareness training (information security awareness training programs in which all employees, agents, and contractors must participate, including, based on job responsibilities, customized education programs that focus on issues regarding use of health information and responsibilities regarding confidentiality and security)		

6. 2 Technical security services to guard data integrity, confidentiality, and availability

Requirement		Implementation features ● = mandatory; ⊙ = at least one required; ○ = optional
Access control	● ⊙ ⊙ ⊙ ○	**A procedure for emergency access** (documented instructions for obtaining necessary information during a crisis) **Context-based access** (an access control procedure based on the context of a transaction as opposed to being based on attributes of the initiator or target) **Role-based access** **User-based access** **Encryption**
Audit controls (mechanisms employed to record and examine system activity)		
Authorization control (the mechanism for obtaining consent for the use and disclosure of health information)	⊙ ⊙	**Role-based access** **User-based access**
Data authentication (The corroboration that data has not been altered or destroyed in an unauthorized manner. Examples of how data corroboration may be assured include the use of a check sum, double keying, a message authentication code, or digital signature.)		

Requirement		Implementation features ● = mandatory; ⊙ = at least one required; ○ = optional
Entity authentication (the corroboration that an entity is the one claimed)	●	**Automatic logoff** (a security procedure that causes an electronic session to terminate after a predetermined time of inactivity, such as 15 minutes)
	●	**Unique user identifier** (a combination name/number assigned and maintained in security procedures for identifying and tracking individual user identity)
	⊙	**Password** **Personal identification number (PIN)** (a number or code assigned to an individual and used to provide verification of identity)
	⊙	**Telephone callback procedure** (method of authenticating the identity of the receiver and sender of information through a series of ‘‘questions’’ and ‘‘answers’’ sent back and forth establishing the identity of each. For example, when the communicating systems exchange a series of identification codes as part of the initiation of a session to exchange information, or when a host computer disconnects the initial session before the authentication is complete, and the host calls the user back to establish a session at a predetermined telephone number)
	⊙	**Token**

6.3 Technical security

Requirement		Implementation features ● = mandatory; ⊙ = at least one required; ○ = optional
Communications or network controls	●	**Integrity controls** (a security mechanism employed to ensure the validity of the information being electronically transmitted or stored)
	●	**Message authentication** (ensuring, typically with a message authentication code, that a message received [usually via a network] matches the message sent)
	⊙	**Access controls** (protection of sensitive communications transmissions over open or private networks so that they cannot be easily intercepted and interpreted by parties other than the intended recipient)
	⊙	**Encryption**
Network controls if a network is used (to protect sensitive communication that is transmitted electronically over open networks so that it cannot be easily intercepted and interpreted by parties other than the intended recipient)	●	**Alarm** (In communication systems, any device that can sense an abnormal condition within the system and provide, either locally or remotely, a signal indicating the presence of the abnormality. The signal may be in any desired form ranging from a simple contact closure (or opening) to a time-phased automatic shutdown and restart cycle)
	●	**Audit trail** (the data collected and potentially used to facilitate a security audit)
	●	**Entity authentication** (a communications or network mechanism to irrefutably identify authorized users, programs, and processes and to deny access to unauthorized users, programs, and processes)
		Event reporting (a network message indicating operational irregularities in physical elements of a network or a response to the occurrence of a significant task, typically the completion of a request for information)